State of Montana Information Security Advisory Council
Minutes
March 8, 2017
1:00 PM
Cogswell Building, Room 151

Members Present:
Ron Baldwin CIO/SITSD, Chair
Lynne Pizzini, CISO/SITSD
Joe Frohlich, SITSD
Stuart Fuller, DPHHS
Jesse Callender, MATIC/Justice
Jon Straughn, COR
General Bryan Fox, DMA
Manuel Soto, OPI
Joe Chapman, DOJ
Craig Stewart, DMA
Kreh Germaine, DNRC
Adrian Irish, UoM
Margret Kauska, Revenue
Erika Billiet, City of Kalispell

Staff Present:
Wendy Jackson

Guests Present:
Craig Stewart, Dave Johnson, Lance Wetzel, Dawn Temple, Daniel Nelson, Rebecca Cooper, Craig Marquardt, Tim Kosena, Sean Rivera

Real-time Communication:
Michael Jares, Bert Quick, Rawlin Richardson, Brad Flath, Billie Byrd, Brian Jacobson, Chris Silvonen, Cheryl Pesta, Channah Wells, Darrin McLean, John Cross, Jerry Kozak, Jim Gietzen, Sky Foster, Zach Day, David Swenson, Phillip English, Erin Stroop, Glynis Gibson, Jessica Plunkett, Larry Krause, Cyndie Lockett, Jerry Marks, Michael Barbere

Welcome and Introductions
Ron Baldwin welcomed the council to the March 8, 2017 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes
Motion: General Bryan Fox moved to approve the February 8, 2017 minutes as presented. Stuart Fuller seconded the motion. Motion passed.

Business
Legislative Session
Lynne Pizzini updated the council on security related legislation. House Bill 61 is an act to revise the 911 laws and establishes the 911 Advisory Council with oversite from the DOA. A hearing on HB 61 is scheduled for March 14, 2017 in the Energy and Telecommunications Committee. Senate Bill 19 would eliminate the statutory requirement to provide an SITSD report to the State Administration and Veterans Affairs Interim Committee (SAVA). The State Administration and Veterans Affairs Interim Committee requested the elimination of this report because it is a duplication of information that is reported to the Legislative Finance Committee (LFC). This Bill was passed in the Senate, transmitted to the house, and failed on the third reading. Several legislators have testified about the need for extensive oversite in Information Technology (IT) due to its high cost and integral nature. Senate Bill 118 would revise the Uniform Fiduciary Access to Digital Assets Act. This Bill gives direction on user disclosure of digital assets and access to electronic communications and content of users. This Bill was transmitted to the House in February 2017, and is moving through the process. Senate Bill 20 would eliminate the requirement of the Court Administrator to prepare an IT report to the Justice Interim Committee. This Bill has been passed in the Senate and transmitted to the House. House Bill 147 would require a search warrant for a government entity to access any personal electronic device. This Bill was transmitted to the Senate and a hearing is scheduled for March 4, 2017. House Bill 148 would revise electronic communications laws to require a search warrant for disclosure of electronic communications by a provider of an electronic communications service. This Bill was transmitted to the House on February 6, 2017. House Bill 149 is an act prohibiting the use of a license plate reader with the exceptions of the Department of

Transportation (DOT) and Law Enforcement. This Bill was transmitted to the House on February 15, 2017. A hearing in the Judiciary Committee is scheduled for March 10, 2017.
Action Item: CIO Support Staff will post the Legislative Report to the ITMC website at http://sitsd.mt.gov/Governance/Boards-and-Councils/ITMC.

National Cyber Security Review – Peer Report
Joe Frohlich stated that the Peer Reports from the National Cyber Security Review (NCSR) have been completed. Both state and local government entities were included in this survey. The council has approved these surveys to be used as the agency self-assessment tool, beginning in November, 2017. Mr. Frohlich reviewed the Peer Reports to provide clarity for agencies utilizing this tool in the future. This report generates an individual score for agencies which reflects their Cyber Security status. These scores are compared against the national average. This report offers a historical perspective which allows agencies to compare current performance to past survey results. These reports will be submitted to the State CIO and a summary will be provided to the Governor. The Enterprise Security Program will collect contact information from each agency regarding the individual designated to complete the NCSR form. This will facilitate the construction of user accounts and allow for a smooth rollout of this review. The Enterprise Security Program will work with the MT-ISAC to develop a guide for agencies outlining how to complete the NCSR survey. There will also be a demonstration in October, 2017 to illustrate how to complete this survey. The NCSR survey will be available to agencies from November 1 to December 31, 2017. Once agencies have completed the NCSR, a final report will be printed, signed by the agency CIO, and submitted to Ron Baldwin. The NCSR reports are confidential and not subject to Freedom of Information Act (FOIA) requests. These reports will only be made available to Legislative auditors if requested. All printed reports must be marked as confidential.

Department of Justice (DOJ) – Phishing Report Outlook Add-in
Daniel Nelson, security analyst with the DOJ, spoke to the council regarding the Phishing Report Outlook Add-in that is being utilized by the DOJ to report suspected Phishing emails. This tool allows all phishing reports to be collected in a central location. The Outlook Add-in adds the email as an attachment and sends it to a predesignated email address. There are several vendors who provide this service including; KnowBe4, PhishMe, and PhishReporter-Outlook-Add-In. Users may also modify Microsoft's Junk Email Reporter add-in, but this sends a report to Microsoft as well. DOJ is utilizing the add-in from KnowBe4 as it is free service and easily customizable. This add-in appears as a button on the user's toolbar and allows suspicious emails to be sent to IT security. The email is then automatically deleted from the user's inbox. This button was added through Microsoft Installer (MSI) and tested on a small user group to ensure it would not affect Outlook performance. The add-in was then pushed out to the rest of the agency. It is up to each agency how they wish to proceed with reporting suspicious emails and phishing.
Kreh Germaine commented that KnowBe4 should be added to the Approved Software list.
Lynne Pizzini stated that an ITPR must be submitted before this can be considered for the Approved Software list.

Data Loss Prevention
Joe Frohlich gave the monthly update on Data Loss Prevention (DLP). Microsoft is working to address an issue with DLP where the tool tip is not delivered, or shows up blank. Known issues with DLP are discussed at the Network Managers Group (NMG) on a weekly basis. Mr. Frohlich has been working with the Enterprise Application Services to create a log for agency security officers to view DLP incident reports. Security officers may only view reports from their agency. This log will be completed and ready for agency use by the end of March, 2017. Dave Johnson stated that this log will be in the reports section of the Exchange Tasks page. DLP reports will contain the email sender, receiver, subject line, and reason the email was blocked. The original email will not be included. The log, once established, will contain reports from the prior 30 days. Agencies will have three months to review this reporting system before DLP goes live on July 1, 2017. This log will help agencies identify areas generating large amounts of blocked emails and provide them training on how to properly send secure information. Mr. Frohlich stated that there have been several requests from agencies for DLP template customization. DLP templates do can be customized specifically for an agency. This customization is difficult and complex. Mr. Frohlich asked the council to approve a no customization request for DLP for the for the first six months after July 1, 2017. This will allow confidence levels to be adjusted appropriately first. Once DLP is turned on, there are two response options for Exchange response to a blocked email. The first message option is limited and cannot be changed. A tool tip will be shown in Outlook and it will

not allow you to send the email. The Enterprise Security Program is not recommending this option. The second option will display the tool tip in Outlook but it will not prevent the user from clicking the send button but the message will not send. The user will then receive a customizable message with a link to the Enterprise Security Program site and contact information. The message response time from the second option is much faster and will result in less confusion for the end user. Mr. Frohlich and Mr. Johnson recommended that the council chose option two as a response for emails blocked by DLP. Mr. Frohlich is actively recruiting live DLP testers from each division within the Department of Administration (DOA). SITSD is creating a document outlining the proper procedures for sharing of sensitive information through DLP File Transfer. Mr. Johnson verified that DLP is only blocking outgoing messages.
Joe Chapman commented that the omission of the original blocked email from this report will extend the amount of time required to verify false positives.
Action Item: Mr. Frohlich will notify agencies when the log is available for use.
Action Item: Mr. Frohlich will notify NMG and MT-ISAC when the DLP Procedures document is complete.
Motion: Lynne Pizzini moved that the MT-ISAC adopt the second message option for DLP, with refinement of the message to be decided later. General Fox seconded the motion. Motion passed.
Mr. Baldwin extended a special thanks to Mr. Johnson, Mr. Frohlich, Mr. Tuman, Mr. Mitschke and staff for their work on DLP.

MT-ISAC Topics of Discussion
Annual DMZ Scan
Sean Rivera spoke to the council regarding the upcoming Annual Demilitarized Zone, or DMZ, Scan which is scheduled to occur in May, 2017. This scan fulfills the requirement, from the National Institute of Standards and Technology (NIST), to conduct vulnerability scanning. The Tenable Nessus Vulnerability scanner will be used to conduct a discovery scan on the DMZ the first night. This helps identify targets for conducting the vulnerability scan the next night. Once vulnerabilities are discovered for remediation, a follow up is conducted. Mr. Rivera requested that the council review the frequency of these scans and consider the benefit of conducting them on a more regular basis. These scans have been streamlined to reduce the disruptive effects on the system. The DMZ scan in 2016 revealed vulnerabilities in 13 agencies. Ms. Pizzini clarified that this scan does not analyze the Web Application Firewall (WAF).
Mr. Fuller suggested that the DMZ scan be conducted on a quarterly basis.
Mr. Baldwin recommended that the frequency of DMZ scans be every 90 days. This change should be documented in a security procedure.
Action Item: Mr. Rivera will draft recommendations, regarding increased frequency of DMZ scans, to be presented to the council in the Aril 12, 2017 MT-ISAC meeting.

Small Cyber Incident Handling Steps
Mr. Frohlich commented that the Incident Categorization Chart in this document has been updated to incorporate recommendations of the MT-ISAC regarding Alert Classifications from Websense.

MT-ISAC Council Members for next Biennium
Mr. Frohlich stated that MT-ISAC member applications will be submitted to the Governor's office in April, 2017. Individuals interested in membership to the MT-ISAC should contact Mr. Frohlich at jfrohlich@mt.gov.

Disposal of Media Storage – Enterprise Offering
Mr. Frohlich is working with the Office of Contracts and Asset Management to establish an Enterprise Offering for the Disposal of Media storage. This will require a Request for Procurement (RFP). Ms. Pizzini requested agency participation on the RFP for this Enterprise Offering. Individuals interested in participating in this RFP should contact Mr. Frohlich at jfrohlich@mt.gov. Agencies can purchase disposal services via this contract. If agencies need disposal services prior to the establishment of this Enterprise Offering, please contact Linda Kirkland at lkirkland@mt.gov to obtain a copy of the SITSD contract.
Mr. Germaine suggested that this contract not be exclusive. This will allow remote locations the flexibility to work with local vendors if necessary.

State Security Conference
Mr. Frohlich spoke to the council regarding the Big Sky Information Security Conference. This is a free event, hosted by the University of Montana, which will be held April 19, 2017 in Missoula. Adrian Irish, with the

University of Montana, recommended that individuals complete registration by March 10, 2017. There has been larger than anticipated interest in this event and registration may need to be closed.

Server Antivirus Update
Mr. Frohlich stated that Enterprise Application Services is still implementing the Server Antivirus update within the SITSD hosted environment. A document is being created to explain the Server Antivirus process. DNRC is installing the Sophos licensing and will test the process and identify potential issues. Once this testing is complete, the Enterprise Security Program will contact agencies to distribute Sophos licenses.
Action Item: Mr. Frohlich will communicate the estimated timeline for the distribution of Sophos licenses to the MT-ISAC once this information is available.

ESP Professional Security Training Grant Winners
Mr. Frohlich stated that there were 16 applicants for the ESP Professional Security Training Grant. Nine individuals were awarded the grant. The winners included tribal members, as well as local and state government employees. Mr. Frohlich congratulated all grant winners.

Workgroup Updates
Best Practices / Tools Workgroup Update
Ms. Pizzini updated the council on recent Best Practices / Tools Workgroup activities. The workgroup has received input on the Acceptable Use – Rules of Behavior document. This document has been updated and posted for review. There will be an Action Item on this document in the April 12, 2017 MT-ISAC meeting.
The Identification and Authentication Best Practices document has been updated and is posted for review. Ms. Pizzini requested that council members review this document and provide feedback to Mr. Frohlich at jfrohlich@mt.gov. If not major revisions are required, there will be an Action Item on this document in the April, 2017 MT-ISAC meeting.
Mr. Germaine requested clarification on the Acceptable Use – Rules of Behavior document.
Rebecca Cooper stated that this is a summary document which includes best practices from NIST and other standardized documents. This document is used as an onboarding guide to inform individuals of expectations regarding acceptable use and behavior. This is intended as supplemental guide that agencies may build upon to incorporate their requirements.
Q: Mr. Germaine: Have the Legal Department and Human Resources reviewed this document?
A: Ms. Pizzini: Yes. Five different agency attorneys have also reviewed the Confidentiality Agreement included within the Acceptable Use – Rules of Behavior document.
Mr. Chapman requested a list of the attorneys who have reviewed this document.
Action Item: Ms. Pizzini will provide Mr. Chapman with a list of the attorneys who have reviewed Acceptable Use – Rules of Behavior document.

Antivirus Augmentation Demos
Ms. Pizzini stated that Antivirus Augmentation demos will be held the week of March 13, 2017.

Situational Awareness / Outreach / Public Safety Workgroup Update
Mr. Frohlich announced that Jesse Callender will replace John Burrell as the MATIC representative. General Fox will become the new Chair of the Situational Awareness / Outreach / Public Safety Workgroup. This meeting will continue to be held at the MATIC the third Wednesday of each month from 10:30 AM to 11:30 AM. Individuals interested in participating in the workgroup should contact Mr. Frohlich at jfrohlich@mt.gov. The outreach letter to state associations has been finalized. The workgroup is compiling a list of addresses. This communication will be sent out once all address information has been gathered.

Current Threats
Sean Rivera gave a brief update of Current Threats. Reports show that, in 2016, Ransomware was present on one out of five emails. The most popular Ransomware variants were Locky, Petya, Cryakl, and Shade. SPAM accounted for 58% of all email traffic in 2016. There were 248 U.S. data breaches through February 28, 2017. Over 1M records were compromised or exposed due to those breaches. Amazon's Simple Storage Service (S3) suffered an outage on February 28, 2017. This outage was due to a typo made during debug maintenance. A study suggested that 94% of critical vulnerabilities released during 2016 could be fixed by removing admin rights. 100% of Edge vulnerabilities were mitigated by removing admin rights.

Action Item: CIO Support Staff will post the Current Threats presentation to the MT-ISAC website (http://sitsd.mt.gov/Governance/ISAC).

Open Forum
Mr. Fuller stated that 2,200 RSA FOBs have been rolled out across the Department of Health and Human Services (DPHHS). This rollout will be completed by the end of march, 2017. This has been a remarkably smooth implementation.
Action Item: CIO Support will add the successful deployment of RSA for DPHHS to the Information Technology Managers Council (ITMC) agenda for the April 5, 2017 meeting.
Future Agenda Items
Mr. Germaine requested a review of SITSD's Ransomware plan.

Public Comment
None

Next Meeting
April 12, 2017
1:00 PM to 3:00 PM
Cogswell, Room 151